Information Technology Standards

Federal Aviation Administration

September 30, 2011

Version 8.4

CHANGE CONTROL CHART

VERSION NUMBER	DESCRIPTION OF CHANGE	DATE
1.0	Draft of Charter – developed outline	06-19-2003
1.1	Refined content in existing sections	07-22-2003
1.2	Re-wrote scope and group charter, added Recommendations section	08-25-2003
1.3	Further editing, added Conclusion section	08-27-2003
1.4	Changed review cycle to monthly, and incorporated recommended wording changes.	09-16-2003
1.5	Revised build-to and buy-to baseline standard. Revised layout of charter to align with the creation of a technical standard.	05-08-2004
1.6	ITEB Cost Control Team 3 comments addressed – quarterly review cycle	06-10-2004
2.0	CIOC Comments addressed	07-07-2004
3.0	Updated Standard	06-16-2005
3.1	Updated for Antivirus Desktop Standard	01–09-2006
3.2	Expanded for servers and network devices	04-27-2006
3.3	Added a laptop standard, updated Adobe Acrobat and WinZip standards; IPV6 language added on network switches; 1 Gig RAM for desktop buy-to standard due to Vista	06-15-2006
4.0	Adds remote access standards, Adds the SQL specification for databases and identifies our build-to standard as Oracle and MS SQL Server. Adds FIPS 140-2 as a specification relating to laptop encryption and identifies Safeboot as our product for doing that. Updates two Sun server models which reached end-of-life. The V240 and V440 are replaced with the V245 and V445 respectively; Adds a standard for Storage Area Networking Added standards citations in several areas (column D), Adds a row on data modeling & identifies ERwin as our build-to standard	04-17-2006
4.1	Adds Sun server X4600 M2 to the list of standards	07-05-2007

CHANGE CONTROL CHART

VERSION NUMBER	DESCRIPTION OF CHANGE	DATE
5	• Adds GIS, Business intelligence/reporting, and video teleconferencing standard • Server virtualization technical and product standard • Dell Servers, Sun servers, and switches are updated. • Desktop operating system – build-to standard updated from Windows 2000 to Windows XP (due to IT Asset Inventory) • Desktop Office Suite – updated build-to from Office 2000 Pro to Office 2003 (due to IT Asset Inventory) • LCD monitor standard added. • Updates versions particularly for software products (MS Project, Adobe Acrobat, Windows Media Player, Visio, and Winzip) • Replaced the Cisco 3500 family of switches with the Cisco 3750 family of switches • Proposed change to waiver process in Section 3 of this document. • Section 8 – addition of OMB requirement for federal desktop security settings • Added Data center utility standards • Adds rationale for several product based standards (response to AGC recommendation) • Adds a build-to standard for network access control	03/05/2008
5.1	Waiver process revised.	04/21/2008
5.2	• Increased desktop RAM requirement; Buy-to increases from 1 GB or higher to 2 GB or higher; Build-to increases from 512K to 1 GB; due to Lotus Notes V8 needs in conjunction with MS Office and the Windows desktop operating system • Removed the Sun V245 and V445 models as they are no longer available from Sun. • Added to our existing Sun server standards the Sun T5140 and T5240 UltraSPARC models due to newer technology offerings from Sun for better performance, scalability and compute density (compact rack size), power & cooling advantages as well as ATO interest. • Updated the Sun X2200 to the Sun X2200 M2 server due to change by Sun	06/24/2008

CHANGE CONTROL CHART

VERSION NUMBER	DESCRIPTION OF CHANGE	DATE
	• Added the Sun X4150 and X4450 Intel Xeon servers. They offer power and cooling advantages, small space requirement, and offer VMWare/ VMotion compatibility with other Intel servers. They are compatible with the Dell Intel servers • Updated the Dell 1950 and the 2950 models to the Dell 1950 III and the 2950 III models due to Dell product line changes • Removed the Dell 6850 model as it is no longer available • Replaced the Dell 6850 (discontinued) with the Dell R900 server, its replacement • Updated the Dell blade server 1955 with the M600 replacement Dell blade server (both Intel chip)	
5.3	Sun server M series added; Hitachi line of storage devices added as an interim standard	7/29/2008
5.4	Windows Server 2008 and Oracle 11g added to buy-to list as part of updating the standards	9/4/2008
6.0	Updated desktop and laptop standard; updated flash standard;	12/18/2008
6.1	Added standards for smart card readers and their middleware; Updated Sun SPARC server standard; Removal of “interim” status for Hitachi storage standard; Added information on contract sources (SAVES, etc.)	2/26/2009
6.2	Revises file compression standard into a file compression/data encryption standard; Changes buy-to standard to encryption products that are FIPS 140-2 compliant including SecureZip	4/16/2009
6.3	Adds IBM System Architect to the build-to standards for “Modeling”; “Data Modeling”; Adds IBM Telelogic Synergy to the build-to standard for Software CM; Adds “IBM System Architect Visio Process Integrator” to the build-to standard for “Business/Technical Diagramming”; Adds a build-to standard for server operating systems; Replaces Sun AMD X4200 server with its life cycle replacement, the X4240.	7/30/2009
6.4	Added SOA standards (separate spreadsheet); Added comment on planned migration to IE8.	8/24/2009
6.5	Added document management build-to standard and double sided copying (rows 23 and 61 of 1st worksheet only)	11/19/09

VERSION NUMBER	DESCRIPTION OF CHANGE	DATE
7.0	Added second set of SOA standards; Added Windows XP SP3 and Lotus Notes 8.02; Updated column on enterprise agreements/contracts; modified wording on double sided printer per ARB request	1/21/2010
7.1	Adds IE8 and Release 2 of Windows Server 2008 to buy-to	2/9/2010
7.2	Adds a 3rd set of SOA standards; Updates Dell servers;	4/22/2010
7.3	Specifies SP3 of MS Office 2003 in the buy-to, more general laptop standard, software vulnerability analysis standards, updates to contracting vehicles and updated comments. Added section 9.0 Technology Related FAA Orders/ Policies/Standards	5/20/2010
7.4	Adds Data Loss Prevention standard (Vontu); Migrates first set of standards to new standards types; Adds NIST 800-53 as a broadly applicable standard in Section 8.	7/15/2010
7.5	Migrates second set of standards to new standards types, adds two more SOA security standards	9/30/2010
8.0	Migrates a third set of standards to new standards types; includes 2 additional SOA security standards (SAML and WS-Security Policy 1.2) and addition of Client Browser plugins category (Flash and Silverlight)	11/18/010
8.1	Further migration of standards to new standards types; updated Current Enterprise Agreements & Contracts values based on SAVES updates from AOT-100; Added Sharepoint 2010 as an emerging standard	1/5/2011
8.2	Adds two requirements management tools (Doors and RequisitePro); Updated standards relating to Citrix, Adobe & Visio; Apple iPad settings, additional sunset dates, migration of standards to new standards types	6/16/2011
8.3	Updates Adobe standards, contract vehicles, drops Synergy as a CM standard	8/18/2011
8.4	Added Progress Savvion as a BPMS standard, Winzip sunset standard, Updated the following: Dell server standards, MS Project, and Lotus Notes versions	

1. Purpose

Under the sponsorship of the CIO and the FAA Architecture Review Board (ARB), Chief Information Officer Council (CIOC), the Technology Control Board (TCB) was tasked with updating agency standards. This is part of the FAA Technical Reference Model (TRM) as described in the Federal Enterprise Architecture Framework (FEAF). Among the driving influences behind the creation of information technology (IT) standards include:

a) A mandate from the Office of Management and Budget (OMB) to manage IT efficiently and effectively
b) FAA and e-Government initiatives to control IT costs
c) Industry success with IT standardization to control IT costs

In effect, standards provide a better means to manage the agency's IT assets. FAA is using IT standards in enterprise-wide procurement vehicles (using larger volume purchases to attain lower industry prices) including enterprise license agreements.

2. Scope

These IT standards apply to Administrative and NAS Regulatory Support (formerly administrative and mission support systems), internal to the FAA, excluding real-time NAS systems relating to air traffic control. In general, these standards specify each standard to a selected level of detail such as a base model or series while allowing the requiring FAA organization or program the flexibility to add options or features available from a vendor for that specified standard.

These standards do not apply to contracts such as performance-based contracts where the FAA has delegated to a contractor the decision-making on the nature of the hardware and software for meeting FAA requirements (for example, the FTI Program's contracts). However, performance based contracts should justify why they are going outside these standards

The standards are defined in terms that are compatible with OMB's Federal Enterprise Architecture (FEA) and the categories outlined in the FEA TRM.

3.0 Waiver Process

While the primary objective is to define standards for use across the FAA's Lines of Business (LOBs) and Staff Offices (SOs), some exceptions to the standard may exist based on the requirements of legacy applications and other legitimate business needs. Exceptions to the standard should not be based on user or organizational preferences. A waiver request from this standard may be approved if it meets one of the following conditions:

a. The standard has a direct measurable negative impact on a service we provide the public.
b. The standard will adversely affect an LOB/SO business or performance goal.

c. The standard will negatively impact business applications or increase costs substantially.

Procedures:

1. Prepare waiver request: The waiver request form is provided in Appendix C. Anyone may file a request. Waivers are needed if one is taking an action that does not conform to either 1) a relevant technical standard cited or 2) an acquisition or “buy-to” standard. If there is no relevant technical or buy-to standard, then no waiver is needed.
    - If the requestor is a manager, skip to the LOB/SO CIO (Step 3).
2. Obtain manager concurrence: The requestor's immediate supervisor must review and concur with the request, and forward it to the LOB/SO CIO.
3. Obtain LOB/SO CIO approval or concurrence: Per the charts below, if the request has a low or very low impact, the LOB/SO CIO must approve or deny the waiver request. Approved requests must be sent to the Chief Technology Officer (ARD-1), the ARB chair, for information. Otherwise, if ARB approval is required, the LOB/SO CIO must review and concur with the request, and forward the request to the ARB chair or designees.
4. Obtain ARB approval: The ARB must review and approve or deny the waiver request. If an expedited approval is required, the ARB chair may act on the request without the full ARB.
5. Analyze approved waiver requests: The ARB chair will analyze the approved waivers in aggregate, looking for trends that will help determine what additional steps are needed to maximize service value, efficiency, and effectiveness.
6. The LOB/SO CIOs will forward their approved waivers to the FAA CIO who will analyze and aggregate the waivers.
7. If the LOB or SO CIO wishes to appeal the ARB decision, the SES official above the CIO may appeal the decision to the ITEB.

Level of Impact of the Proposed Waiver to FAA Technical Reference Model (TRM) and/or FAA IT Standards

Impact Level	Description
Very High	Waiver involves a national application of technology or cross-FAA or new platform or E-Gov or high business impact; Or the waiver involves ISS implications
High	Involves Major LOB or cross-LOB application of technology or standards; $10M and above (lifecycle cost) or time critical or management directed; Or the waiver involves ISS implications
Medium	Moderate LOB application of technology or standard; Or waiver involves an investment that exceeds $1M in cost; And the waiver has minor or no ISS implications
Low	Scope is limited to a subset of an LOB or less than 500 employees or less than 10 servers or less than 100 desktops; And waiver has minor or no ISS implications; Or the wiaver duration is for less than 15 months and the waiver does not impede future competition among vendor products
Very Low	Waiver is intended for a short duration of less than 10 months; And the waiver has minor or no ISS implication; And the waiver involves costs of less than $250K and does not impede future competition among vendor products

[Minor or no ISS implications refers here to a low probability of a risk or threat and a low severity of potential outcome from such risk(s) or threat(s)].

Program Impact	**Reviewers**	**Approvers**
Very High	Manager, LOB/SO CIO	ARB
High	Manager, LOB/SO CIO	ARB
Medium	Manager	LOB/SO CIO
Low	Manager	LOB/SO CIO
Very Low	Manager	LOB/SO CIO

Any waivers granted from the above process only apply to FAA IT Standards and FAA's Technical Reference Model (TRM). It does not apply to other kinds of standards such as data standards described in FAA Order 1375.1D.

4.0 Information Technology Standards

Appendix A enumerates the specific standards within the Federal Technical Reference Model framework. FAA is currently transitioning to an expanded lifecycle standards types so two standards tabs are being maintained during the transition - Appendix A – IT Standards and Appendix A – New Types. The tab called "Appendix A - IT Standards" portrays the standards in three categories – Relevant International/Government standards, FAA minimum (or build-to) standards and FAA acquisition standards (or buy-to) standards. The tab called “Appendix A – New Types standards” expands the technology lifecycle into four lifecycle types – Emerging, Current, Contained, and Sunset. (Note that the standards listed in both Appendix A tabs are not a requirement for all configurations to have all of the software listed. For instance, many desktops will not have Microsoft Project or Visio software).

For Appendix A – IT Standards, the following lifecycle definitions apply:

Relevant International/Government Standards

- These are internationally recognized standards that the FAA is targeting for compliance in its target architecture. These standards apply to the acquisition (or “buy-to”) standards; they do not relate to the “build-to” standards.
- Sources for these standards include the International Organization for Standardization (ISO), International Electro-technical Commission (IEC), National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF), and others.

Characteristics of FAA Minimum Standards – Build-To Standards

- These standards are meant to be the target environment for software applications being currently built for national fielding across FAA organizations within the next 10 months. They recognize the current installed base of hardware and software at the FAA. They are used to simplify development and ensure successful deployment by providing a stable and predictable infrastructure.
- These hardware and software standards often represent the norm in the FAA. They represent an average or below average system in the FAA.
- With few exceptions, we intend that current applications are compatible with the build-to standard, especially enterprise-wide applications.

Characteristics of FAA Acquisition Standards – Buy-To Standards

- Meaning: If an LOB or SO is to make a purchase in the near future, then they are expected to purchase the buy-to standard or seek a waiver.
- The standard ought to support an economically efficient system life. For desktops, this is about 3-4 years for a desktop system (shorter for any laptop hardware standards) as determined by the FAA LOB or SO.
- Constraint: These standards need to be a currently commercially available product or one that is anticipated to be available shortly or within the target time horizon of the standard.

For Appendix A – New Types tab, the following Lifecycle definitions apply:

Emerging Standards

- These are new technologies that have the potential to become current. These technologies have been identified as potential candidates to fulfill future FAA technology needs. While emerging, early adopters of the technology must be carefully considered.

- This category is intended to give developers and system integrators an advanced indication of what emerging technologies are likely to be considered to replace existing functionality.

Current Standards

- When a technology is current, it is part of the FAA standards. Information systems targeting deployment of new systems during the timeframe listed should use that technology. Other technologies will require waivers.
- Current standards do not limit the use of contained standard technologies for existing systems.
- Contained Standards -Contained standards are technologies that are no longer considered a current standard, but are still in use because of compelling business reasons. Contained technologies should be replaced with current technologies as soon as feasible. No new information systems will use "contained" technologies.

Developers and system integrators are still required to maintain support for contained standards

Sunset Standards

- Sunset standards consist of technologies that are no longer considered a current standard, but may still be in use because of compelling business reasons.
- Sunset Technologies in use past the sunset date will require a waiver to continue to operate on FAA networks.
- Sunset technologies should be replaced with current technologies as soon as feasible. No new information systems will use "sunset" technologies.
- (The Sunset standard category provides a projected date for developers and system integrators on when support for a specific technology can be discontinued.)

The Scope column in Appendix A – New Types is used to describe the scope of a standard as being FAA-wide or NRSA.

5.0 Future Updates.

Due to the changing nature of technology, these standards are updated periodically through the TCB with ARB approval.

6.0 Mechanism to test standards.

In order to promote the integration of standards in desktop and server environments and compatibility with agency applications, FAA testing capabilities may be required to properly test changes to the standards. Some testing capabilities exist in the FAA already. Where possible, FAA organizations ought to use existing testing facilities within the LOBs.

7.0 Standard Compliance

FAA organizations are expected to follow these standards in any new systems unless a waiver is obtained from the LOB/SO CIO. Furthermore, forthcoming life cycle controls in the Acquisition Management System are expected to call for program managers to make use of the Enterprise architecture at several stages of their acquisition process. The latter includes compliance with FAA's Technical Reference Model (TRM) which includes this standard.

8.0 Broadly Applicable Standards

The following are standards with a broad scope affecting virtually all federal information technology.

A) The Federal Information Processing Standard (FIPS) Publications 199 and 200 have broad applicability for federal information and federal information systems. The NIST authored these in February 2004 and March 2006 respectively. They were issued as a result of the Federal Information Security Management Act (FISMA).

- FIPS Publication 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.
- The FIPS 200 standard addresses the specification of minimum security requirements for federal information and information systems. It is applicable to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2)

B) National Institute for Standards and Technologies (NIST) Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

- NIST SP 800-53 specifies recommended Security Controls for Federal Information Systems and Organizations

C) Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they shall ensure that the electronic and information technology allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. The FAA Acquisition Management System (AMS)

Rehabilitation Act policy mandates that after June 21, 2001, new procurements (contracts, task orders, delivery orders, orders under government wide-schedules, interagency agreements) shall include requirements that have provisions for Electronic and Information Technology (EIT) Accessibility Standards (for telecommunication products, information kiosks, transaction machines, web sites, multimedia, office equipment and others.) Please refer to Appendix B, when procuring EIT, and insert the 36 Code of Federal Regulations for the applicable commodity.

D) OMB requirement for Implementation of Commonly Accepted Security Configurations for Windows Operating Systems [sometimes referred to as the Federal Desktop Core Configuration (FDCC)] - OMB Memo M-07-11, March 22, 2007 – Agencies are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS). This applies primarily to desktop and laptop computer systems. Further information is at NIST web sites (currently http://csrc.nist.gov/fdcc/) within FAA, contact your ISSM for more information.

9.0 Technology Related FAA Orders/Policies/Standards

There are many technology related FAA Orders or Policies. For the latest versions of these, see the relevant FAA web sites including:

1) FAA Employee Web site's Orders and Notices site (https://employees.faa.gov/tools_resources/orders_notices/).
2) Many of them are posted at the AIO Intranet site in its Library section (as of March 2010 at https://intranet.faa.gov/faaemployees/org/staffoffices/aio/library/).
3) Another source of technology-related standards focusing more on the NAS but sometimes more broadly applicable are at the Air Traffic NAS Standards web site (as of March 2010 at http://www.faa.gov/air_traffic/nas/system_standards/standards/) .

Some examples of technology related FAA orders and standards as of March 2010 are:

- FAA-STD-063, FAA Standard Practice, XML Namespaces
- FAA-STD-064. FAA Standard Practice, Web Service Registration
- FAA-STD-065: Standard Practice: Preparation Of Web Service Description Documents
- FAA-STD-066: Standard Practice: Web Service Taxonomies
- FAA Order 1375.1D Information/Data Management and FAA Data Governance Board
- ISS Program Policy (1370.82A)
- Internet Access Points Policy (1370.83)
- Internet Services Policy (1370.84)
- Information Operations Condition (1370.89)
- Internet Access Point Configuration Management (1370.90)
- ISS Patch Management (1370.91)
- Password and PIN Management (1370.92)
- Wireless Technologies Security Policy (1370.94A)
- Wide Area Network Connectivity Security (1370.95)

- Media Sanitizing and Destruction Policy (1370.100)
- System Use Notification and Disclaimer Statement Policy (1370.102)
- Encryption Policy (1370.103)
- Digital Signature Policy (1370.104)
- Logical Access Control Policy (1370.105)
- Information Systems Security Awareness and Training Policy (1370.106)
- Rules of Behavior/System Use Policy (1370.107)
- FAA Information Technology (IT) Standards
- Information Security C&A Handbook and Templates
- ISS Standard Baseline Configuration Resources

Appendix A – FAA Information Technology Standards

See matrix of hardware and software standards.

Appendix B – Section 508 Standards

The electronic and information technology (EIT) Section 508 standards are as follows:

CFR 1194.21 –Software applications and operating systems
CFR 1194.22—Web-based information or applications
CFR 1194.23---Telecommunication products
CFR 1194.24—Video and Multimedia products
CFR 1194.25---Self contained, closed products (e.g., information kiosks, calculators, copiers, and fax machines
CFR 1194.26---Desktop and Portable Computers
CFR 1194.31---Functional Performance Criteria
CFR 1194.41---Information, Documentation and Support

If you procure, develop, maintain or use the below commodities, please insert the corresponding standard(s) in your procurement documents. In all cases, for each commodity, 1194.41 Information, Documentation and Support should be inserted, as well.

EIT Commodity	Section 508 Standard(s)
Application Servers	**1194.21** Software applications and operating systems
Business/Technical Diagramming	**1194.21** Software applications and operating systems
Collaboration/Communication-Electronic Mail	**1194.21** Software applications and operating systems
Collaboration/Communication-Instant Messaging	**1194.21** Software applications and operating systems
Desktop Suite	**1194.21** Software applications and operating systems
Electronic Channels-Terminal Communications	**1194.21** Software applications and operating systems
File Compression	**1194.21** Software applications and operating systems
Graphics	**1194.21** Software applications and operating systems
Integrated Development Environment	**1194.21** Software applications and operating systems
Internet/Intranet Web sites	**1194.22** Web-based Intranet and Internet Information and Applications
Media Servers	**1194.21** Software applications and operating systems
PDF/Creation	**1194.21** Software applications and operating systems
Peripherals/Video Card	**1194.24** Video and Multimedia Products
Peripherals/CD Creation	**1194.21** Software applications and operating systems

EIT Commodity	Section 508 Standard(s)
Platform Independent	**1194.21** Software applications and operating systems
Portal Servers	**1194.21** Software applications and operating systems
Project Management	**1194.21** Software applications and operating systems
Servers/Computers	**1194.26** Desktop and Portable Computers
Software Configuration Management	**1194.21** Software applications and operating systems
Test Management	**1194.21** Software applications and operating systems
Wireless/Mobile	**1194.21** Software applications and operating systems
Web Servers	**1194.21** Software applications and operating systems
Web Browser	**1194.21** Software applications and operating systems
Wireless/PDA	**1194.25** Self-contained, closed products

Appendix C – REQUEST FOR WAIVER FROM FAA TECHNICAL REFERENCE MODEL (TRM) AND/OR INFORMATION TECHNOLOGY STANDARDS

1) Requestor's Name ___________________________ 2) LOB ______ 3) Org Acronym_____

4) Work Address____

5) Nature of waiver:

6) Indicate the standard or TRM component that the waiver is for: (technical standard and/or buy-to standard)

7) If the waiver is limited to a certain period of time for purchasing non-standard items, state the duration until (month/year):_____________

8) Does the waiver have information systems security implications? YES NO (circle one)
If yes, describe them as high, medium or low. Minor or no ISS implications refers here to a low probability of a risk or threat and a low severity of potential outcome from such risk(s) or threat(s).
Explain why:

9) Costs related to waiver (cost of HW or SW to be bought as a result of waiver; Or cost of overall investment related to waiver) $___________
Describe costs: ____

____

10) Does the waiver require ARB approval? YES NO
Waivers require ARB approval depending on their impact. See IT Standards document (section 3) for description of impact levels and which ones involve a waiver that require ARB approval.
If the waiver does not require ARB approval, then the CIO may approve.

11) Requestor signature and date____
Expedited approval requested YES NO

12) Optional – Supervisor concurrence, date____________________________________

13) CIO Signature and date____

14) ARB approval and date____
(ARB co-chair or secretariat)

15) If denied, denial rationale: ____

For questions, contact AIO/ARD-300